DRAFT

Unofficial

1. (Amended) A computer-implemented method for securely transmitting an information package from a sender to an addressee via a network, the method comprising the steps of:
determining whether the addressee has a public key;
in response to the addressee not having a public key:
encrypting the package with an escrow encryption key;
storing the package in escrow for the addressee;
notifying the addressee of the package in escrow; and
in response to receiving an acknowledgement from the addressee:
issuing new public and private keys to the addressee; and
in response to subsequently verified authentication of the addressee:
transmitting the package to the addressee via the network.

2. (Original) The method of claim 1, wherein the step of determining whether the addressee has a public key comprises the sub-step of:
checking a public key directory for a public key of the addressee.

3. (Original) The method of claim 1, further comprising the step of:
storing the addressee's new public key in a public key directory.

4. (Original) The method of claim 1, wherein the encrypting step comprises the sub-steps of:
providing an escrow encryption key and an escrow decryption key,
wherein the escrow encryption and decryption keys comprise one of symmetric keys and asymmetric keys; and
encrypting the package with the escrow encryption key.

5. (Amended) The method of claim 1, wherein the notifying step comprises the sub-step of:
sending a notification to the addressee via the network, wherein said nofitication includes an attached module for generating private and public keys at the addressee location.

6. (Original) The method of claim 5, wherein the notification comprises one of an e-mail notification, a desktop notification, a voice notification, a pager notification, and a facsimile notification.

7. (Original) The method of claim 1, further comprising the step of:
decrypting the package with an escrow decryption key corresponding to the escrow encryption key.

8. (Original) The method of claim 1, wherein the escrow encryption key is different from the new public and private keys issued to the addressee.

9. (Original) The method of claim 1, wherein the acknowledgement from the addressee includes an indication of the addressee's name and e-mail address.

DRAFT

10. (Original) The method of claim 1, further comprising the step of:
in response to an address having a public key;
encrypting the package with the addressee's public key;
storing the package;
notifying the addressee of the package;
authenticating a user as the addressee by manipulating a message sent by the addressee encrypted using the addressee's private key; and
transmitting the package to the authenticated addressee in response to authenticating the user as the addressee.

11. (Canceled) The method of claim 1, wherein the step of transmitting the package comprises the sub-steps of:
authenticating the user as the addressee; and
transmitting the package to the authenticated user via the network.

12. (Original) A computer implemented method for securely transmitting an information package to an addressee via a network, the method comprising the steps of:
determining whether the addressee has a public key;
in response to the addressee not having a public key:
encrypting the package with an escrow encryption key;
storing the package in escrow for the addressee;
notifying the addressee of the package in escrow; and
in response to receiving an acknowledgement from the addressee:
issuing new public and private keys to the addressee;
decrypting the package with an escrow decryption key;
re-encrypting the package using the addressee's new public key; and
transmitting the package to the addressee via the network.

13. (Original) The method of claim 12, wherein the step of determining whether the addressee has a public key comprises:
checking a public key directory for a public key of the addressee.

14. (Original) The method of claim 12, further comprising the step of:
storing the addressee's new public key in a public key directory.

15. (Amended) The method of claim 12, wherein the step of transmitting the package comprises the sub-steps of:
authenticating the user as the addressee by evaluating a message encrypted by addressee; and
transmitting the package to the authenticated user via the network.

16. (Original) The method of claim 12, further comprising the step of:
decrypting the package using he addressee's new private key.

DRAFT

17. (Amended) A system for securely transmitting an information package to an addressee via a network, the system comprising:

a directory interface adapted to check a directory to determine whether the addressee has a public key;

an escrow manager, coupled to the directory interface, adapted to provide an escrow encryption key for encrypting the package;

an encryption module, coupled to the escrow key manager, adapted to encrypt the package with the escrow encryption key;

a computer-readable medium, coupled to the encryption module, adapted to store the package in escrow for the addressee;

a notification module, coupled to the computer-readable medium, adapted to send a notification to the addressee via the network;

a key registration module, coupled to the notification module, adapted to issue, in response to the addressee acknowledging the notification, new public and private keys to the addressee; and

a transmission module, coupled to the key registration module and to the computer-readable medium, adapted to transmit the package to the addressee via the network in response to successful decryption of a message sent by addressee using the new public key of addressee.

18. (Original) The system of claim 17, further comprising:

a directory coupled to the directory interface, adapted to store a public key of at least one addressee.

19. The ~~method~~ system of claim 18, wherein the key registration module is further adapted to store the addressee's new public key in the directory.

20. (Original) The system of claim 17, wherein the notification module is adapted to send one of an e-mail notification, a desktop notification, a voice notification, a pager notification, and a facsimile notification.

21. (Original) The system of claim 17, wherein the escrow key manager is adapted to provide an escrow decryption key, the system further comprising:

a decryption module, couple to the transmission module, adapted to decrypt the package using the escrow decryption key.

22. (Original) The method of claim 21, wherein the escrow encryption key and the escrow decryption key comprise one of symmetric keys and asymmetric keys.

23. (Original) The system of claim 17, wherein the directory interface and the encryption module are each adapted to operate within a sending system; wherein the computer-readable medium, the notification module, and the transmission module are each adapted to operate within a server system; and

wherein the key registration module and the decryption module are each adapted to operate within a receiving system.

DRAFT

24. (Original) The system of claim 23, wherein the key registration module is received by the receiving system as an attachment to a notifcation.

25. (Original) The system of claim 23, wherein the key registration module is received by the receiving system by following a hyperlink in a notification.

26. (Original) The system of claim 23, wherein the transmission module within the server system is adapted to transmit the package in escrow to the decryption module within the receiving system; and wherein the decryption module within the receiving system is adapted to receive the package from the transmission module, receive an escrow decryption key manager, and decrypt the package with the escrow decryption key.

27. (Amended) The system of claim 23, wherein the transmission module within the server system is adapted to receive an escrow decryption key from the escrow key ~~manger~~ manager, decrypt the package in escrow using the escrow decryption key, receive the addressee's public key from a directory, re-encrypt the package using the addressee's public key, and transmit the package to the decryption module within the receiving system; and wherein the decryption module within the receiving system is adapted to receive the package from the transmission module, retrieve the addressee's private key from the key registration module, and decrypt the package using the addressee's private key.

28. (Amended) In a computer-readable medium, a computer program product for securely transmitting an information package to an addressee via a network, the computer-readable medium comprising program code adapted to perform the steps of:

determining whether the addressee has a public key;
in response to the addressee not having a public key;
encrypting the package with an escrow encryption key;
storing the package in escrow for the addressee;
notifying the addressee of the package in escrow; and
in response to receiving an acknowledgement from the addressee:
~~issuing~~ transmitting a new public and private keys generation module to the addressee;
issuing new public and private keys at addressee's location; and
contingnet upon authentication of the addressee based on a message sent by address subsequent in time to the acknowledgement received from the addressee, transmitting the package to the addressee via the network.

29. (New) The method of claim 1, wherein said step of authentication of the addressee includes the sub-steps of:

the addressee encrypting a message using addressee' private key;
the addressee sending said private-key encrypted message to the server;
the sender decrypting said private-key encrypted message using addressee's public key;
the sender authenticating the addressee based on the content of the decryption of said private-key encrypted message.

DRAFT

30. (New) The method of claim 1, wherein said step of authentication of the addressee includes the sub-steps of:

the addressee requesting registration with a certificate authority;

the certificate authority registering the addressee subsequent to verifying at least one of the addressee's name, address, telephone number, e-mail address;

the certificate authority generating at least a public key associated with the addressee;

the certificate authority making the public key available for use by the sender; and

the sender authenticating the addressee based on decryption of a message using the public key.